ACTA ARITHMETICA
X (1964)

Sur les progressions arithmétiques et géométriques formées de trois nombres pseudopremiers distincts

par

A. Rotkiewicz (Varsovie)

On appelle pseudopremiers les nombres composés n, tels que $n \mid 2^n-2$. W. Sierpiński a posé le problème s'il existe des progressions arithmétiques formées de trois nombres pseudopremiers distincts. Je démontrerai ici les théorèmes suivants:

Théorème 1. *Il existe une infinité de progressions arithmétiques formées de trois nombres pseudopremiers distincts.*

Le théorème 1 résulte tout de suite du théorème suivant:

Théorème 2. *Il existe une infinité des nombres naturels n tels que les nombres n, $2n-1$ et $3n-2$ sont pseudopremiers.*

Lemme. *Si n, $2n-1$ et $3n-2$ sont des nombres pseudopremiers impairs et $3 \nmid n(2n-1)$, alors pour $N = \dfrac{2^{2n-1}+1}{3}$, les nombres N, $2N-1$ et $3N-2$ sont pseudopremiers et on a $3 \nmid N(2N-1)$.*

Démonstration du lemme. Supposons que n, $2n-1$ et $3n-2$ sont des nombres pseudopremiers impairs. On a alors $2n-1 = n_1 n_2$, où $n_1 > 1$, $n_2 > 1$, $2 \nmid n_1 n_2$. On a

$$N = \frac{2^{2n-1}+1}{3} = \frac{2^{n_1 n_2}+1}{3} = \frac{2^{n_1}+1}{3} \cdot \frac{2^{n_1 n_2}+1}{2^{n_1}+1},$$

où, d'après $n_1 > 1$, $n_2 > 1$, $2 \nmid n_1 n_2$, toutes les deux fractions sont des nombres entiers > 1. On a

$$2N-1 = \frac{2^{2n}-1}{3} = \frac{2^n+1}{3}(2^n-1),$$

où, vu que $n > 1$ et $2 \nmid n$, tous les deux facteurs sont des entiers > 1, et

$$3N-2 = 2^{2n-1}-1 = 2^{n_1 n_2}-1, \quad 2^{n_1}-1 \mid 2^{n_1 n_2}-1,$$

où, d'après $n_1>1$ et $n_2>1$ on a $1<2^{n_1}-1<2^{n_1n_2}-1$. Les nombres N, $2N-1$ et $3N-2$ sont donc composés. On a $N-1=\frac{2(2^{2n-2}-1)}{3}$.

Les nombres impairs n et $2n-1$ étant pseudopremiers, on a $n \mid 2^{n-1}-1 \mid 2^{2n-2}-1$ et $2n-1 \mid 2^{2n-2}-1$. Vu que $3 \nmid n(2n-1)$, on a donc $2n(2n-1) \mid N-1$. Il en résulte que

$$N=\frac{2^{2n-1}+1}{3} \mid 2^{2(2n-1)}-1 \mid 2^{N-1}-1,$$

$$2N-1=\frac{2^{2n}-1}{3} \mid 2^{2n}-1 \mid 2^{N-1}-1 \mid 2^{2N-2}-1,$$

$$3N-2=2^{2n-1}-1 \mid 2^{N-1}-1 \mid 2^{3N-3}-1$$

(cf. [3]) et les nombres N, $2N-1$ et $3N-2$ sont des nombres pseudopremiers impairs.

Comme $3 \nmid 2n-1$, on a $2n-1=6k+r$, où k est un entier $\geqslant 0$ et $r=1$ ou 5, d'où $2^{2n-1}+1=2^{6k+r}+1 \equiv 2^r+1 \not\equiv 0 \pmod 9$, donc $3 \nmid \frac{2^{2n-1}+1}{3}=N$. Pareillement, vu que $3 \nmid 2n$, on a $2n=6t+r$, où t est un entier $\geqslant 0$ et $r=2$ ou 4, d'où $2^{2n}-1=2^{6t+r}-1 \equiv 2^r-1 \not\equiv 0 \pmod 9$ et $3 \nmid (2^{2n}-1)/3=2N-1$. On a donc $3 \nmid N(2N-1)$ et le lemme se trouve démontré.

Démonstration du théorème 2. Vu le lemme, il reste à trouver un nombre naturel n tel que les nombres n, $2n-1$ et $3n-2$ soient pseudopremiers impairs et tels que $3 \nmid n(2n-1)$. Je dis qu'un tel nombre est $n=\frac{2^{37}+1}{3}$. En effet, on a $n=\frac{2^{37}+1}{3}=1777\cdot 25781083$, $2n-1=\frac{2^{38}-1}{3}=174763\cdot 524287$, $3n-2=2^{37}-1=223\cdot 616318177$. Les nombres n, $2n-1$ et $3n-2$ sont donc composés. Or, on a $n-1=\frac{2(2^{36}-1)}{3}$ et, vu que $2\cdot 19 \mid 2(2^{18}-1)$, $2^{18}-1 \mid 2^{36}-1$, on a $2\cdot 19 \mid n-1$ et, comme $37 \mid 2^{36}-1$, on a $2\cdot 37 \mid n-1$. On a donc $n=\frac{2^{37}+1}{3} \mid 2^{2\cdot 37}-1 \mid 2^{n-1}-1$, $2n-1=\frac{2^{2\cdot 19}-1}{3} \mid 2^{2\cdot 19}-1 \mid 2^{n-1}-1 \mid 2^{2n-2}-1$, $3n-2=2^{37}-1 \mid 2^{n-1}-1 \mid 2^{3n-3}-1$. Les nombres n, $2n-1$ et $3n-2$ sont donc pseudopremiers. Le théorème 2 est ainsi démontré.

Il est à remarquer que dans le théorème 1 le mot *pseudopremiers* peut être replacé par le mot *premiers*, mais la démonstration est alors beaucoup plus difficile (voir [1]). Or, on ne sait pas si le théorème 2 reste

vrai lorsqu'on y remplace le mot *pseudopremiers* par le mot *premiers*. La réponse positive résulte d'une hypothèse de L. E. Dickson (voir [2]).

Pareillement comme nous avons démontré le théorème 2 (mais d'une façon plus longue) on peut démontrer le

Théorème 3. *Si n et $2n-1$ sont des nombres pseudopremiers impairs et $(n(2n-1), 2^{2^k+1}-1)=1$ alors le nombres*

$$\frac{2^{2^k(2n-1)}+1}{2^{2^k}+1}, \quad \frac{2^{2^{k+1}n}-1}{2^{2^{k+1}}-1}, \quad \frac{2^{2^k(2n-1)}-1}{2^{2^k}-1} \qquad \text{où} \quad k=0,1,2,\ldots$$

sont pseudopremiers et forment une progression arithmétique.

Pour $k=0$ on obtient les nombres $\frac{2^{2n-1}+1}{3}$, $\frac{2^{2n}-1}{3}$ et $2^{2n-1}-1$, c'est-à-dire les nombres N, $2N-1$ et $3N-2$ de la démonstration du théorème 2.

Voici encore un triple de nombres pseudopremiers formant une progression arithmétique

$$\frac{2^{26}+1}{5}=53\cdot 157\cdot 1613, \quad \frac{2^{28}-1}{15}=29\cdot 43113\cdot 127, \quad \frac{2^{26}-1}{3}=2731\cdot 8191.$$

Théorème 4. *Il existe des progressions géométriques formées de trois nombres pseudopremiers distincts.*

Démonstration du théorème 4. Telle est la progression géométrique formée des nombres a, $a\cdot 1093$ et $a\cdot 1093^2$, où

$$a=\frac{2^{182}+1}{1093^2(2^{14}+1)(2^{26}+1)}.$$

On peut vérifier que a est un nombre naturel composé et que $364 \mid a-1$, d'où $a \mid 2^{182}+1 \mid 2^{364}-1 \mid 2^{a-1}-1$ et a est un nombre pseudopremier. Or, comme $364 \mid 1092$, on a $364 \mid a-1$, $1093a-1=1093(a-1)+1092$, donc $364 \mid 1093a-1$, d'où $1093a \mid 2^{182}+1 \mid 2^{364}-1 \mid 2^{1093a-1}-1$. Pareillement on trouve que $1093a^2 \mid 2^{364}-1 \mid 2^{1093a^2-1}-1$. Les nombres a, $a\cdot 1093$ et $a\cdot 1093^2$ sont donc pseudopremiers.

Une autre progression géométrique formée de trois nombres pseudopremiers distincts est celle qui est formée des nombres $\frac{a}{4773}$, $\frac{a}{4773}\cdot 1093$ et $\frac{a}{4773}\cdot 1093^2$. Je ne sais pas s'il existe une infinité de progressions géométriques formées de trois nombres pseudopremiers distincts.

Travaux cités

[1] S. Chowla, *There exists an infinity of 3-combinations of primes in A.P.*, Proc. Lahore Philos. Soc. 6 (2) (1944), pp. 15-16.

[2] L. E. Dickson, *A new extension of Dirichlets theorem on prime numbers*, Messenger of Math. 33 (1904), pp. 155-161.

[3] W. Sierpiński, *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n-2)/n$, Coll. Math. 1 (1947), p. 9.

Reçu par la Rédaction le 18. 1. 1964

ACTA ARITHMETICA
X (1964)

Über die Nichtlinearität einer gewissen Gruppe

von

W. Fluch (Göttingen)

In [1] wurde bewiesen, daß jede beschränkte, endliche Darstellung der Gruppe $G = \{a, b, c, d\}$ mit den Relationen

$$(1) \qquad b^{-1}ab = a^2, \quad c^{-1}bc = b^2, \quad d^{-1}cd = c^2, \quad a^{-1}da = d^2$$

trivial ist. Wir wollen dieses Ergebnis verschärfen und zeigen, daß jede endliche Darstellung von G trivial ist; damit ist dann die Nichtlinearität der Gruppe vollständig bewiesen. Als Korollar hat man folgenden

Satz 1. *Es gibt Gruppen* $(\neq 1)$ *mit endlich vielen Erzeugenden und Relationen, deren sämtliche endliche Darstellungen trivial sind* [1].

Ein etwas schwächerer Satz wurde in [1] (Satz 8) bewiesen. Der hier bewiesene Satz stellt auch eine Verschärfung eines bekannten Theorems von Fuchs-Rabinowitsch [2] dar, welches besagt, daß es Gruppen mit endlich vielen Erzeugenden und Relationen gibt, welche nicht isomorph einer Matrixgruppe sind. Zum Beweis benötigen wir eine Verbesserung von Lemma 3 aus [1] in folgender Form

Lemma 1. *Gibt es zu einer endlichen invertierbaren Matrix* U *eine invertierbare Matrix* V, *sodaß* $V^{-1}UV = U^t$ *(mit* $|t| \geqslant 2$, *ganzrat. Zahl) gilt, so sind alle Eigenwerte von* U *Einheitswurzeln. Hat* U *unendliche Ordnung, dann hat* V *mindestens einen Eigenwert* $|\lambda| \neq 1$ *(genauer: dann hat* V *mindestens zwei Eigenwerte* λ_1, λ_2 *mit* $\lambda_2 = \lambda_1 t$*).*

Bevor wir dieses Lemma beweisen, zeigen wir wie daraus das behauptete Ergebnis folgt. Sind nämlich $\bar{a} = D(a), \bar{b}, \bar{c}, \bar{d}$ die den Erzeugenden a, b, c, d zugeordneten Matrizen bei einer beliebigen endlichen Darstellung D von G, so folgt aus den Relationen (1) und dem ersten Teil des Lemmas das Zwischenresultat

[1] Zusatz bei der Korrektur: Die Klasse der endlich-erzeugbaren Gruppen, welche keine nichttriviale endlich-dim. Darstellung besitzen, wird in meiner demnächst erscheinenden Arbeit *Gruppen ohne endlich-dimensionale Darstellungen* angegeben.